

## IDENTITY THEFT PREVENTION

### Identity Theft

- NEVER carry your Social Security card on your person. Store it in a safe place.
- Give your Social Security number ONLY WHEN NECESSARY. Always ask to use an alternate type of identification.
- NEVER give personal information over the telephone unless you initiate the call.
- NEVER answer unsolicited email requests for personal information even if the source appears legitimate.
- Request and review your credit bureau reports ANNUALLY from ALL three credit reporting agencies (Experian, Equifax, and TransUnion). Credit bureaus are not in the business of protecting personal information. They are in the business of making a profit by collecting and selling information. They are not required to verify this information with consumers. For example, an imposter can change your address by filing a change of address card with the post office. The credit bureau will change their files to reflect your "new" address without verifying it with you first. The "new" address is sold to financial institutions, marketing firms, and insurance companies who then fill your imposter's mailbox with pre-approved applications in your name.
- PLACE PASSWORDS on all of your financial accounts such as bank, credit cards, telephone, cell phone, and investment accounts. Change the passwords about every six months. Do not carry a list of your PIN numbers or passwords on your person. Refrain from using your mother's maiden name as a password. In addition, NEVER give your mother's maiden name when applying for credit. Most institutions will accept an alternate identifier. Your child's name, spouse's name, or pet's name are also unsafe passwords. NEVER use your address, date of birth, or any portion of your Social Security number as a PIN or password. Safe passwords or PIN numbers are a combination of letters, numbers, and symbols. Avoid using consecutive letters or numbers such as abcd or 1234.
- DO NOT give personal information over a cell or portable phone. These transmissions are easily monitored.
- KNOW the date you should receive your bank and credit card statements. A missing statement could indicate a thief has changed your address and diverted your mail. Contact the bank or credit card company immediately.
- REVIEW your bank and credit card statements immediately upon receipt to detect unauthorized transactions.
- CHECK your telephone and cell phone bills for calls you did not make.
- CARRY only the credit cards that are necessary. Cancel the cards you do not use.
- KEEP personal papers in a safe place.
- TAKE outgoing mail to the post office. Do not leave mail unattended in an outside, open, or unsecured mailbox.
- PROMPTLY remove mail from your mailbox once it has been delivered.
- STOP mail while on vacation.
- SHOP only with the online merchants you know. Many e-businesses are extensions of brick-and-mortar establishments. Remember that online shopping is no different than shopping off-line. You will find reputable and disreputable businesses in both worlds. Even if you know the merchant, make sure the site is secure before entering your credit card information. The URL, or web site address, should begin with "https." A graphic, such as a lock, should appear in the bottom right corner of your browser bar.
- Before ordering online, read the company's privacy policy. If a privacy policy does not exist, contact the company and request one. This information is vital. You need to know how they intend to use your personal information.
- NEVER give your bank account numbers or Social Security number to an online merchant.
- USE a low-limit credit card for online shopping.
- CHECK the Better Business Bureau's website for information about the company before shopping online. Look for the BBB Online Reliability Seal on the website.
- REPORT your identity theft to the police and the Federal Trade Commission (FTC).

### Lost Purse or Wallet

If you have lost your purse or wallet in the Town of Vienna, the Police Department wishes to assist you in every way possible. Since your purse/wallet (containing various items of personal identification, credit cards, and checks) was lost, you are at risk for criminal victimization through personal identity theft. Personal identity theft sometimes begins with a lost or stolen purse or wallet.

Personal identity theft is the unauthorized use of another person's personal identifying information to: obtain credit, goods, services, money, or property; or commit a felony or misdemeanor. Personal identifying information means a person's name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings or checking account number, or credit card number.

We are concerned with ensuring that you take appropriate steps to decrease your chance of becoming a victim of identity theft. We suggest the following:

- Purchase a large notebook and begin by making notations about the date, time, location, and other important information regarding the loss of your belongings.
- It is likely that you will need to make several telephone calls to protect yourself from becoming a victim of identity theft. For each call, record the date, time, telephone number, person's name, purpose of call, what was accomplished, what follow-up is needed, and other relevant notes. Also, write down any questions you asked and the answers received.
- Keep copies of all letters you write and all forms you submit. Mail everything by certified mail. Keep these records in a safe place. Be consistent and methodical, and take action immediately! Begin by contacting all three credit report bureaus.
- Contact the three major credit bureaus: TransUnion, Experian, and Equifax. Request that a fraud alert be placed on your file immediately. You will be assigned a reference or confirmation number to use in future communications. Your name and address will be removed from prescreened mailing lists for a length of time specified by each credit bureau. Each credit bureau is different, so follow their instructions explicitly. They may ask you to [write a letter](#) and enclose copies of three pieces of identification before they mail your report. Be sure to ask how long the alert will be in effect and how to extend it, if necessary.

#### [EQUIFAX](#)

Business Hours: Monday through Friday, 9:00 a.m. - 5:00 p.m.  
Telephone: 1-800-525-6285 or 1-888-766-0008

#### [EXPERIAN](#)

Business Hours: Monday through Friday, 9:00 a.m. - 5:00 p.m.  
Telephone: 1-888-397-3742 or 1-800-311-4769

#### [TRANSUNION](#)

Business Hours: Monday through Friday, 8:30 a.m. - 4:30 p.m.  
Telephone: 1-800-680-7289

Order a copy of your credit report from each of the credit bureaus every three to six months for the first year. After the first year, order copies semi-annually or at least annually. Remember, if the person(s) who stole your identity has not been apprehended and/or your belongings have not been recovered, your identity still remains in their possession and you are subject to future victimization. Or, your imposter may have sold your information to someone else who may attempt to use it at some later date.

If your ATM or Debit Card has been lost, report this theft to your bank. Close this account and open a new account number and new password. Do not use your old password. Act quickly to ensure that you are not held liable for the fraudulent funds obtained by your imposter.

If checks were lost, cancel the accounts immediately. Notify your bank of the number and payee on the last check you wrote. Place "stop payments" on the remaining checks. Ask your bank to notify the check verification company they use. Here is a list of some of these companies:

National Check Fraud Service: 1-843-571-2143

CrossCheck: 1-800-843-0760

Equifax Check Systems: 1-800-437-5120

International Check Services: 1-800-526-5380

SCAN: 1-800-262-7771

TeleCheck: 1-800-710-9898

Chex Systems: 1-800-428-9623

It may be necessary that YOU contact the major check verification companies. If so, request each company to notify retailers in their database to not accept the lost checks.

If your driver license has been lost, apply for a duplicate at a Department of Motor Vehicles. Identification documents are required to issue a replacement license, such as a certified birth certificate, etc. Contact the DMV for a complete list of acceptable documents and specific requirements. Please be aware that photocopies and facsimiles are not adequate proof. Only original documents will be accepted.

When a customer is requesting a replacement driver's license because their license has been stolen, we indicate this on the customer's record as the reason for the replacement. The customer would need to contact law enforcement to report the license as stolen.

DMV also has a Web site you can visit for information on protecting your identity. If you would like to visit that site, it is listed it below.

<http://www.dmv.state.va.us/webdoc/citizen/drivers/identitytheft.asp>

Change the locks on your home and car if your keys were lost. Remember, if someone finds your keys in conjunction with your personal information, they have both your address and access to your residence.

If you have any additional questions, or if you believe you may be a victim of identity theft, please contact the Vienna Police Department for additional instructions.